International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 30 العدد
July 2022 يوليو

Secure data transfer using image steganography

Farhat M.A. Zargoun, Retaj Alnaami, Azhar Aboushagour

Faculty of Information Technology, University of Tripoli
fzargoun@gmail.com

الملخص

يعد الأمن والخصوصية من أهم القضايا في أنظمة الاتصال اليوم. في التطبيقات التي لا يمكن الاستغناء فيها عن أهمية خصوصيتك، يكون الهدف الرئيسي هو إرسال النص إلى الهدف المطلوب دون أن يتم التقاطه من قبل الأشخاص الآخرين.

في هذا البحث اقترحنا خوارزمية لإخفاء النص، حتى لو تم حفظه في ملف نصي، في ملف صورة الغلاف، للخوارزمية المقترحة مرحلتين، الأولى تقوم بتشفير النص باستخدام خوارزمية RSA ، وبعد ذلك تقوم بإدراج النص المشفر نص في ملف صورة الغلاف باستخدام تقنية البت الأقل أهمية (LSB). تم تنفيذ واختبار الخوارزمية المقترحة باستخدام C # .net، وقد أظهرت نتائجنا كفاءة العمل المقترح في إخفاء النص في الصورة واسترجاعه.

الكلمات الدالة: إخفاء المعلومات، التشفير، LSB، RSA ، الاتصال الآمن

Abstract

Security and privacy are the most important issues in today's communication systems. In applications where the importance of your privacy is indispensable, the main aim is to send the text to desired target without being captured by the third persons.

In this paper, we have proposed an algorithm to hide text, even if it saved in text file, in cover image file, the proposed algorithm has two stages, first, it encrypts the text using RSA algorithm, after that, it inserts the encrypted text in cover image file using The Least Significant Bit (LSB) technique. The proposed algorithm has been implemented and tested by using C#.net, our results have shown the efficiency of proposed work in hiding the text in an image and retrieve it.

Keywords: steganography, encryption, LSB, RSA, secure communication.

Introduction

Information security is a science specialized in securing information circulated over the Internet from the risks that threaten it. With the technology development and the means of storing and exchanging information in different ways, or the so-called transfer of data over networks from one location to another, the security of that data and information has become an obsession and a very important topic. Information security can be defined as the science that works to provide protection for information from the risks that threaten it or the barrier that prevents attacking it by providing the necessary tools and means to protect information from internal or external risks. Standards and procedures taken to prevent information from getting into the hands of unauthorized persons through communications and to ensure the authenticity and the communications' authenticity [1].
Steganography is defined as the art of communication, which uses to hide text message into a different forms of cover files, image, audio, or video in order not to leave any trace.
The efficiency of a steganography procedure is measured utilizing three key criteria, payload efficiency, image excellence calculation, and degree of protection [2].
This paper is concentrated on image steganography which is extremely accepted in the steganography field. The Least Significant Bit (LSB) approach is mainly the effectual method employed to entrench the undisclosed communication.
The goal of steganography is keep others from knowing hidden information, in addition, to keep others from thinking that the information even exists. If a used method of steganography causes someone to suspect that a medium carries data, then the method has failed.
Encryption and Steganography achieve separate goals, encryption is changing the meaning of the message so it cannot be read, steganography does not change the meaning or change the data to make it unusable or unintended, and rather, it prevents the third party from suspecting that there is a communication or data even

exists. For some people who want to reach ultimate in security or privacy, can combine both approaches,(see figure (1)), encryption and steganography.

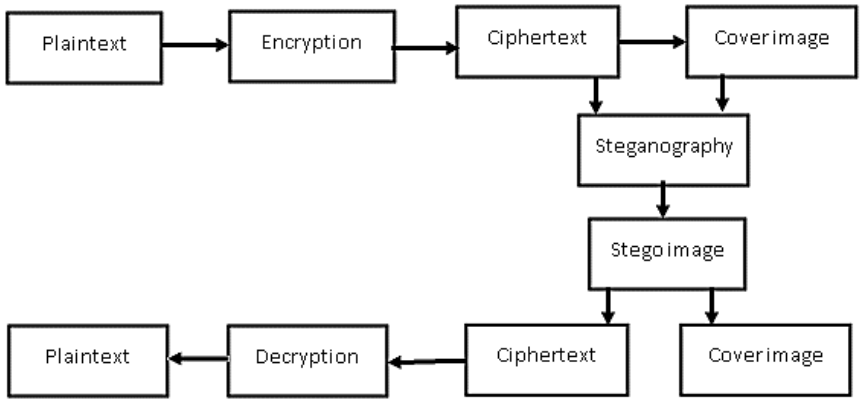

Figure 1 Combination Cryptography and Steganography

Encrypted data is difficult to be differentiate from normal occurring phenomena than a normal plain text (which is a raw text) in the medium; there are several steganography tools that can encrypt data before hiding them in a chosen medium [3].

Related Works

Trivedi and Rana [7] presents about Steganography is put into practice of hiding secret message or the secret information within further multimedia data so as to is text, the image, audio or the video. The power of steganographic method lies in its capacity to remain the message as covert as likely and also quantity of information so as to can be concealed, as huge as possible. In spite of fact that many approaches by now exist in the steganography researches are going away on in the field. This paper gives a survey on the methods used in this area.

Isla et al. [8] presents about the rapid development of data communication in modern era emends secure exchange of information. Steganography is reputable process for hiding data on or after an unauthorized access. Steganographic techniques hide

secret data in different file formats such as: image, text, audio, and video. In this paper, a new image steganography method based on nearly each one major bit (MSB) of image pixels is proposed. Moreover, the presented method is not simply secure, but computationally proficient as well.

THE PROPOSED ALGORITHM

There are three stages should be applied to implement the proposed method:

Stage 1: Hash-LSB (Least Significant Bit) Process

The Hash based Least Significant Bit (H-LSB) technique for steganography in which position of LSB for hiding the secret data is determined using hash function.

Hash function finds the positions of least significant bit of each RGB pixel's and then message bits are embedded into these RGB pixel's independently. Then hash function returns hash values according to the least significant bits present in RGB pixel values [4], [5].

The cover image will be broken down or fragmented into RGB format, then the Hash LSB technique will uses the values given by hash function to embed or conceal the data.

In this technique the secret message is converted into binary form as binary bits; each 8 bits at a time are embedded in least significant bits of RGB pixel values of cover image in the order of 3, 3, and 2 respectively.

According to this method 3 bits are embedded in red pixel LSB, 3 bits are embedded in green pixel LSB and 2 bits are embedded in blue pixel LSB as illustrated in next figure, these 8 bits are inserted in this order because the chromatic influence of blue color to the human eye is more than red and green colors.

Therefore, the distribution pattern chooses the 2 bits to be hidden in blue pixel. Thus the quality of the image will be not sacrificed. Following formula is used to detect positions to hide data in LSB of each RGB pixels of the cover image.

$$k = p \% n \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where, k is the LSB bit position within the pixel; p represents the position of each hidden image pixel and n is the number of bits of LSB which is 4 for the present case.
After embedding the data in cover image, a stego-image will be produced. The recipient of this image has to use the hash function again to extract the positions where the data has been stored. The extracted information will be in cipher text. After decryption of it, combining of bits into information will produce the secret message as required by the
Receiver [6].

Figure 2. Hash-LSB Process

Stage 2: RSA Encryption and Hash-LSB Encoding

A. RSA algorithm can be implemented as follows:

Choose two large prime no. p & q.
Calculate N=p*q
Calculate f(z)=(p-1)*(q-1)Find a random number e satisfying 1 < e < f (n) and relatively prime to f (n) i.e., gcd (e, f (z)) = 1.
Calculate a number d such that d = e-1 mod f (n).
Encryption: Enter message to get cipher text. Ciphertext c= mod ((message. ^e), N). - Decryption: The cipher text is decrypted by : Message=mod ((c. ^d), N).

B. Bedding Algorithm:

Step 1: Choose the cover image & secret message.
Step 2: Encrypt the message using RSA algorithm.
Step 3: Find 4 least significant bits of each RGB pixels from cover image.

Step 4: Apply a hash function on LSB of cover image to get the position.
Step 5: Embed eight bits of the encrypted message into 4 bits of LSB of RGB pixels of cover image in the order of 3, 3 and 2 respectively using the position obtained from hash function given in equation 1.
Step 6: Send stego image to receiver.

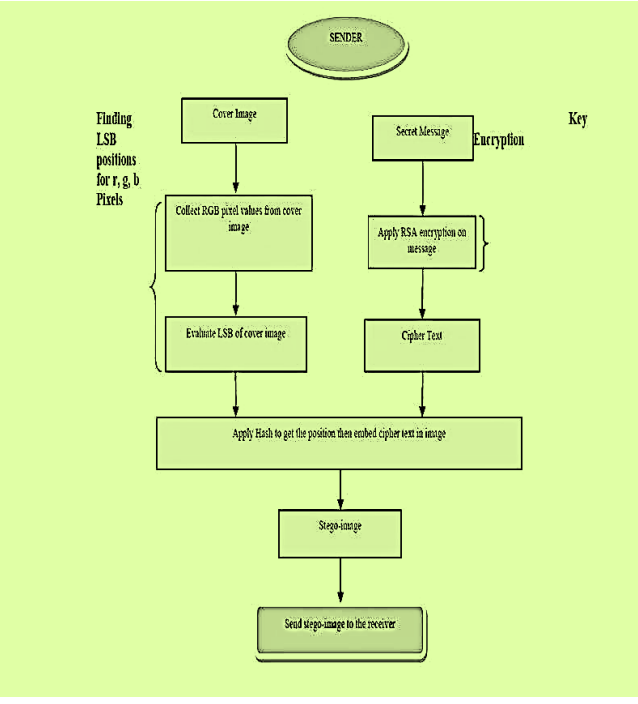

Figure 3 LSB Encoding and RSA Encryption Flow Chart

Phase 3: Hash –LSB Decoding and RSA Decryption
4.6.1 Retrieval Algorithm:
Step 1: Receive a stego image.
Step 2: Find 4 LSB bits of each RGB pixels from stego image.
Step 3: Apply hash function to get the position of LSB's.
Step 4: Retrieve the bits using these positions in order of 3, 3, and 2 respectively.
Step 5: Apply RSA algorithm to decrypt the retrieved data.
Step 6: Finally read the secret message.

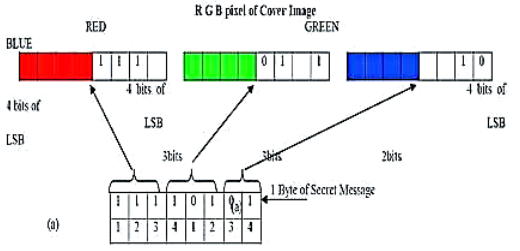

Figure 4 RGB pixel for cover image

Figure 5 LSB Decoding and RSA Decryption Flow Chart

Conclusion

To hide confidential information cryptography and steganography can be effectively used.

In this paper LSB and RSA have been propsed. Along with RSA algorithm the over system becomes more secure. The objective of any Steganographic method is to hide the maximum secret information which is immune to external attacks and also should not

convey the fact that the cover medium is carrying a secret information. This paper helped us understand how data can be passed secretly through an image and how image processing and cryptographic algorithms can be applied for achieving this.
Steganography is in the early stage of development. Several new techniques are being discovered and implemented. It is discovered that time is not far away when its importance would be realized by organizations in general, and armed forces in particular.

REFERENCES

[1] Moh'd Zoghoul. Hussein Hatamleh , Ziad Alqadi, , Muhammed Mesleh, Belal Ayyoub, Jamil Al-azzeh, A comparative analysis of Huffman and LZW methods of color image compression decompression: International Journal of Engineering Science Invention, 2019, Volume 8, Issue 04.

[2] Jamil Al-Azzeh, Bilal Zahran , Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh, A Novel Based on Image Blocking Method toEncrypt-Decrypt Color; INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION 2019, Volume 3 Issue 1.

[3] Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al- Azzeh; Qazem Jaber, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation, Journal of Computer Science and Information Technology,2019, Volume 8 Issue 3.

[4] Ziad Alqadi; Bilal Zahran; Qazem Jaber; Belal Ayyoub; Jamil Al-Azzeh, Enhancing the Capacity of LSB Method by Introducing LSB2Z Method; International Journal of Computer Science and Mobile Computing,2019, Volume 8 Issue 3.

[5] Ahmad Sharadqh, Belal Ayyoub, Ziad Alqadi, Jamil Al-azzeh; Experimental investigation of method used to remove salt and pepper noise from digital color image, International

Journal of Research in Advanced Engineering and Technology,2019. Volume 5 Issue 1.

[6] Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh, Qazem Jaber, Modified, Inverse LSB Method for Highly Secure Message Hiding, International Journal of Computer Science and Mobile Computing,2019, Volume 8 Issue 2.

[7] Himani Trivedi and Arpit Rana, "A Study Paper on Video Based Steganography", International Journal of Advance Research, Ideas and Innovations in Technology, Vol. 3, No. 1, pp. 493-499, 2017.

[8] Ammad Ul Islam et al., "An Improved Image Steganography Technique based on MSB using Bit Differencing", Proceedings of IEEE 6th International Conference on Innovative Computing Technology, pp. 1478-1485, 2016.